35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

SmartSwitch Router
System Firmware Version 3.0.1.0
March, 2000

INTRODUCTION:

This document provides specific information for version 3.0.1.0 of the system firmware for the SmartSwitch Router family of products.

It is recommended that one thoroughly review this release note prior to the installation or upgrade of this product.

FIRMWARE SPECIFICATION:

Before installing the 3.0.1.0 firmware, upgrade the Boot PROM image on the SmartSwitch Router to Boot PROM version 1.1.0.8.

Refer to the SmartSwitch Router Getting Started Guide for instructions on loading the boot PROM software.

Firmware Image Name	Version No.	Type	Release Date
ssr3010	3.0.1.0	Maintenance	March 2000
ssr3002	3.0.0.2	Maintenance	November 1999
ssr3000	3.0.0.0	Customer	October 1999
ssr2220	2.2.2.0	Maintenance	September 1999
ssr2201	2.2.0.1	Customer	May 1999
ssr2200	2.2.0.0	Customer	April 1999
ssr2101	2.1.0.1	Maintenance	February 1999
ssr2100	2.1.0.0	Customer	December 1998
ssr2000	2.0.0.0	Customer	November 1998
ssr1200	1.2.0.0	Customer	September 1998
ssr1100	1.1.0.0	Customer	August 1998
ssr1010	1.0.1.0	Customer/Maintenance	June 1998
ssr1000	1.0.0.0	Customer	April 1998

HARDWARE COMPATIBILITY:

This firmware version is supported on all hardware revisions of the SmartSwitch Router family.

Part	Description	Minimum Firmware Version	Minimum Bootprom Version
SSR-16	16-slot SmartSwitch Router Chassis, Backplane and Modular Fan	1.2.0.0	1.1.0.2
SSR-2-B SSR-2-B-AA	SSR 2000 Base Configuration with 16 10/100 TX ports	1.2.0.0	1.1.0.2
SSR-2-FX /SSR-2-FX-AA	8-port 100 Base-FX module with MT-RJ fiber connectors for SSR 2000	2.1.0.1	1.1.0.2
SSR-2-GSX	SSR 2100 with 8 1000Base-SX ports	2.2.0.1	1.1.0.5
SSR-2-LX SSR-2-LX-AA	SSR 2000 2-port 1000Base-LX Expansion Module	1.2.0.0	1.1.0.2

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

Part	Description	Minimum Firmware Version	Minimum Bootprom Version
SSR-2-LX70 SSR-2-LX70-AA	One port 70 Km 1000Base-LX module MB for SSR 2000	2.0.0.0	1.1.0.2
SSR-2-PKG SSR-2-PKG-AA	SSR 2000 with 24 10/100 TX ports and 2 1000 SX ports	1.2.0.0	1.1.0.2
SSR-2-SER SSR-2-SER-AA	Dual port Serial module for SSR 2000 (No compression or encryption)	2.1.0.0	1.1.0.2
SSR-2-SERC SSR-2-SERC-AA	Quad port Serial module with compression for SSR 2000	2.1.0.0	1.1.0.2
SSR-2-SERCE SSR-2-SERCE-AA	Quad port Serial module with compression and encryption for SSR 2000	2.1.0.0	1.1.0.2
SSR-2-SX SSR-2-SX-AA	SSR 2000 2-port 1000Base-SX Expansion Module	1.2.0.0	1.1.0.2
SSR-2-TX SSR-2-TX-AA	SSR 2000 8-port 10/100 TX Expansion Module	1.2.0.0	1.1.0.2
SSR-8	8-Slot SmartSwitch Router Chassis, Backplane and Modular Fan	1.0.0.0	1.0.0.0
SSR-CM-128	Control Module with 128 MB	1.0.0.0	1.0.0.0
SSR-CM2-128	Revised Control Module with 128 MB	1.1.0.0	1.1.0.2
SSR-CM2-64	Revised Control Module with 64 MB	1.1.0.0	1.1.0.2
SSR-CM-64	Control Module with 64 MB	1.0.0.0	1.0.0.0
SSR-GLX19-02	2-Port 1000 LX (Gigabit) Module (SCLX for MMF or SMF) with 4 MB	1.0.0.0	1.0.0.0
SSR-GLX29-02 SSR-GLX29-02-AA	2-Port 1000 LX (Gigabit) Module (SCLX for MMF or SMF) with 16 MB	1.0.0.0	1.0.0.0
SSR-GLX70-01 SSR-GLX70-01-AA	One port 70 Km 1000 Base-LX module with 16 MB for SSR 8000 and SSR 8600	2.0.0.0	1.1.0.2
SSR-GSX11-02	2-Port 1000 SX (Gigabit) Module (SCSX for MMF Only) with 4 MB	1.0.0.0	1.0.0.0
SSR-GSX21-02 SSR-GSX21-02-AA	2-Port 1000 SX (Gigabit) Module (SCSX for MMF Only) with 16 MB	1.0.0.0	1.0.0.0
SSR-HFX11-08	8-Port 100 FX Module (MMF SC) with 4 MB	1.0.0.0	1.0.0.0
SSR-HFX21-08 SSR-HFX21-08-AA	8-port 100 Base-FX MMF module with 16 MB	1.0.0.0	1.0.0.0
SSR-HFX29-08 SSR-HFX29-08-AA	8-port 100 Base-FX SMF module with 16 MB	2.0.0.0	1.1.0.2
SSR-HSSI-02 SSR-HSSI-02-AA	Dual port HSSI module for SSR 8000 and SSR 8600	2.1.0.0	1.1.0.2
SSR-HTX12-08 SSR-HTX12-08-AA	8-Port 10/100 TX Module (Cat 5 RJ-45) with 4 MB	1.0.0.0	1.0.0.0
SSR-HTX22-08 SSR-HTX22-08-AA	8-Port 10/100 TX Module (Cat 5 RJ-45) with 16 MB	1.0.1.0	1.0.0.0
SSR-PS-16	Power Supply for SSR 8600	1.2.0.0	1.1.0.2
SSR-PS-8	Power Supply Module for SSR 8000	1.0.0.0	1.0.0.0
SSR-SERC-04 SSR-SERC-04-AA	Quad port Serial module with compression for SSR 8000 and SSR 8600	2.1.0.0	1.1.0.2
SSR-SERCE-04 SSR-SERCE-04-AA	Quad port Serial module with compression and encryption for SSR 8000 and SSR 8600	2.1.0.0	1.1.0.2
SSR-SF-16	Switching Fabric Module for SSR 8600	1.2.0.0	1.1.0.2

Note: The SSR-CM2-64/128 Control Modules replace the SSR-CM-64/128 Control Modules. The SSR-CM2-64/128 Control Modules have a 10/100Base-TX management port (as opposed to a 10Base-T port on the SSR-CM-64/128 Control Modules). Otherwise, the functionality of the SSR-CM2-64/128 Control Modules is identical to that of the SSR-CM-64/128 Control Modules.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

BOOT PROM COMPATIBILITY:

The minimum boot PROM version supported for this firmware release is 1.1.0.8. The boot PROM resides in the internal flash on the Control Module. Its primary function is to load the firmware image. Please refer to the 1.1.0.8 Boot PROM release notes for more detail.

For the **SSR 8000**, the following table lists the Control Module and PROM image compatibility for this firmware release.

Control Module	PROM Image
SSR-CM-64 SSR-CM-128	prom-1108cm
SSR-CM2-64 SSR-CM2-128	prom-1108cm2

For the **SSR 8600**, the following table lists the Control Module and PROM image compatibility for this firmware release.

Control Module	PROM Image
SSR-CM2-64 SSR-CM2-128	prom-1108cm2

For the **SSR 2000**, the following table lists the PROM image compatibility for this firmware release.

SSR Part Number	PROM Image
SSR-2-B SSR-2-B-AA SSR-2-PKG SSR-2-PKG-AA	prom-1108ssr2

For the **SSR 2100**, the following table lists the PROM image compatibility for this firmware release.

SSR Part Number	PROM Image
SSR-2-GSX	prom-1108ssr2

NETWORK MANAGEMENT SOFTWARE SUPPORT:

NMS Platform	Version No.	Module No.
CoreWatch	3.0	N/A
SPECTRUM	5.0	Rev. 1
SPMA (Spectrum Portable Management Application)	Post 3.2	Rev. 1
SPEL (Spectrum Element Manager)	2.2	N/A

If you install this image, you may not have control of all of the latest features of this product until the next version(s) of network management software. Please review the software release notes for your specific network management platform for details.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

SUPPORTED FUNCTIONALITY:

Features and Enhancements in 3.0.1.0 Firmware

DHCP
Multiple DNS servers with DHCP - New functionality to serve 3 DNS servers within a DHCP request has been added to this release of the SSR firmware.

VFS2 support
This firmware supports new VFS2 file system. PCMCIA cards with VFS1 take about 10 - 20 minutes to complete an image add or delete operation. With the new VFS2, this operation takes only fraction of the time. Because of the new block allocation mechanism in VFS2, Firmware 3.0.1.0 and BootProm image 1.1.0.8 is required for VFS2.

Server Load Balancing Enhancement

Intrinsic Persistence Checking
In addition to simple source IP persistence, we offer a brand new feature, netmask persistence. You can now select a netmask value from 1 to 32, which is applied against the incoming source IP address. If a binding between the resulting value and a real server already exists, then the client is sent to the same server. Otherwise, the selected load balancing algorithm is used and a server is selected for the client. This solves the mega-proxy problem where a client comes in through a proxy doing NAT translation on their address, which potentially can assign them different addresses during a session. These addresses fall within a specified range for each proxy. By masking off the lower bits of the IP address, you guarantee that all addresses, hence all sessions from a client, go to the same server. This is tied with the new feature of sticky port persistence. If a client already has a binding to a server on one port, such as 80 for HTTP traffic, and starts another application on a different port, such as 443 for SSL secure transactions, the client session will go to the same server for both ports.

For the above features, and for other persistence and binding modes, we have added in timeouts by group, not just for all bindings. Also we have added a feature to allow the selection of the maximum number of concurrent sessions allowed on any given server. This ensures that servers do not get overloaded.

Comprehensive Server Checking
The real server checking routines have been enhanced to allow sending strings (such as ftp, http, smtp an so on) to either the port of the load balanced server or to a different port number on the same server and check the return string against expected values. For example, balance on SSL, but check on HTTP. Another use is to send a request to execute a CGI to test out the entire server, as well as make requests on any backend servers and respond positively only if everything is working correctly. This comprehensive server checking may also be applied across multiple ports (if a server is set to load balance both HTTP and SSL, the HTTP request can check for both HTTP and SSL aliveness).

VPN Load Balancing
Ability to load balance VPN devices running IPSEC. Most devices handshake using port 500 as UDP packets. They then send the data in raw IP format. We have added the ability to load balance based on the first handshake packet to create a binding between the source IP and the real VPN device. Any other packets from the same source location, with the Virtual IP of our Virtual VPN are sent to the same real VPN device, regardless of the fact that the data is coming in as a raw IP stream.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

Features and Enhancements in 3.0 Firmware:

WAN Encryption/Compression
The software supports encryption and compression on the following line cards:

- SSR-SERCE-04 / SSR-SERCE-04-AA
- SSR-2-SERCE / SSR-2-SERCE-AA

Compression only is supported on the following line cards:

- SSR-SERC-04 / SSR-SERC-04-AA
- SSR-2-SERC / SSR-2-SERC-AA

Compression
The Serial boards use LZS compression with a maximum of 64 full-duplex histories. The LZS algorithm has been standardized by many organizations, including ANSI (X3.241) and the Frame Relay Forum (FRF.9). According to the LZS format, the last byte of a compressed stream is always part of the End Marker, and it will be zero approximately 88% of the time. Sometimes this extra byte at the end of the compressed stream is eliminated (called STRIP0 mode).

To be compliant with the ANSI X3.241-1994 compression format standard, the SSR ***never*** strips the last byte. However, in order to be compatible with existing systems supporting this feature, the SSR when necessary inserts a zero in the decompression operation just before the check field or at the end of the compressed data stream if there is no check field.

For PPP, the SSR can support sequence numbers checks. For Frame Relay, the SSR can support sequence numbers and LCB checks.

Encryption
The Serial boards with encryption support the DES encryption format. The SSR supports separate transmit and receive encryption keys. The DES encryption key is configurable through the CLI. This key is 8 bytes of which only 7 bytes (56 bits) are actually used.

Single-DES is supported in 3.0 release.

Important: The encryption feature requires that the SSR be ***physically*** secure. The encryption keys are stored in the SSR, and it is important to keep the SSR console and telnet access protected.

WAN STP
WAN STP is an extension of the existing STP (802.1d compliant) to include WAN ports (PPP, MLP and Frame Relay). The interface is the existing STP CLI commands. To enable STP on a Frame Relay VC, user needs to specify the VC number along with the port.

WAN Multilink PPP (MLPPP)
For 3.0, the WAN software supports multilink PPP (MLPPP) for both HSSI and serial boards. This feature is supported in software and no new hardware is required.

The MLPPP implementation is based on the RFC 1990 specification, which includes:

- Encapsulation:
  Both long format and short format are supported. The default is long format.

· Fragmentation and Reassembly:
Small packets are sent in a round-robin fashion among the member links. Large packets are fragmented into pieces and are distributed evenly among the member links. The size of the fragments is calculated based on the link speed.

WAN Interoperability with Other Cabletron Products
The following tables summarize the compatibility between the SmartSwitch Router 2000/8000/8600's WAN modules and other Cabletron SmartSwitch Router product. The Software and Hardware column describe how those features are supported in that product.

SmartSwitch Router 510/520, software version 4.0:

	Software	Hardware
Compression Control Protocol (CCP)	Yes	N/A
Encryption Control Protocol (ECP)	Yes	N/A
Multi-Link Point to Point Protocol (MLP)	Yes	N/A

CyberSwitch 400, software version 2.1.9:

	Software	Hardware
Compression Control Protocol (CCP)	Yes	Yes

WAN Interoperability with Other Vendors' Products
The following tables summarize the compatibility between the SmartSwitch Router 2000/8000/8600's WAN modules and other vendors' products. The Software and Hardware column describe how those features are supported in that product.

Cisco 7200, software version 11.3:

	Software	Hardware
Compression Control Protocol (CCP)	Yes	No, Cisco bug # CSCdm30601
Encryption Control Protocol (ECP)	No (Proprietary Protocol)	No (Proprietary Protocol)
Multi-Link Point to Point Protocol (MLP)	Yes	N/A
Compression over Frame Relay (FRF.9)	Yes	No, Cisco bug # CSCdm30601

Bay Networks (Nortel) BLN, software version 13.2:

	Software	Hardware
Compression Control Protocol (CCP)	Not tested	Not tested
Encryption Control Protocol (ECP)	No (Proprietary Protocol)	No (Proprietary Protocol)
Multi-link Point tot Point Protocol (MLP)	Yes	N/A
Compression over Frame Relay (FRF.9)	No (Proprietary Protocol)	No (Proprietary Protocol)

Policy based routing
The SSR supports routing packets based on user defined policies. It is a process whereby the router puts packets through a policy before routing them. The policy determines which packets are routed to which router next. You might enable policy routing if you want certain packets to be routed some way other than the obvious shortest path. Policy routing provides the user flexibility and control to define the packet forwarding path based on any or

all fields of the L3/L4 IP headers and user defined policies. Policies can be defined to route packets to a set of next hop IP addresses based on one or many of the following IP header fields:

- IP protocol
- Source IP address
- Destination IP address
- Source Socket
- Destination Socket
- Type of service

RMON/RMON2

Full RMON (RFC 1757) and RMON2 (RFC 2021) are implemented on a per port basis. Version 3.0 firmware supports the following RMON groups:

- Ethernet Statistics Group
- Ethernet History Group
- Alarm Group
- Event Group
- History Control Group
- Host Group
- HostTopN Group
- Matrix Group
- Filter Group
- Packet Capture Group

In addition, version 3.0 firmware adds support for RMON2 including:

- Protocol directory
- Protocol distribution
- Address mapping
- Network layer host
- Network layer matrix
- Application layer host
- Application layer matrix
- User history
- Probe configuration

The SSR RMON/RMON2 feature can be set by the administrator to enable various levels of support: "lite", "standard", and "pro". The administrator can enable "lite", "standard", and/or "pro" based on a specified port list. For example, the administrator can set "lite" on ports et.1.(1-8) and then set "standard" on the same set of ports. RMON "lite", "standard" or "pro" ***cannot*** be set individually on a set of ports. To turn on "standard", user must turn on "lite" and to turn on "pro", user must turn on "standard" and "lite".

Setting RMON "lite" on a set of ports adds support for:

- Ethernet Statistics Group
- Ethernet History Group
- Alarm Group
- Event Group

Setting RMON "standard" on a set of ports adds support for:

- History Control Group
- Host Group
- HostTopN Group

- Matrix Group
- Filter Group
- Packet Capture Group

Routed traffic will not be accounted for in Host Group and Matrix Group.

Setting RMON "pro" on a set of ports adds support for:
- Protocol directory
- Protocol distribution
- Address mapping
- Network layer host
- Network layer matrix
- Application layer host
- Application layer matrix
- User history
- Probe configuration

Bridge traffic will not be accounted for in Network layer host, Network layer matrix, Application layer host, Application layer matrix and Protocol distribution.

RMON/RMON2 Memory Requirements

RMON/RMON2 memory usage on an SSR is configured dynamically based on the number of ports configured with RMON "lite", "standard" or "pro". When RMON/RMON2 is enabled on the SSR 8000/8600, it is recommended to have minimum 128 MB of memory in the Control Module.

The following describes the memory usage for RMON/RMON2 on a per port basis.

	Memory Requirement (Kbytes)
Base Initialization	500
Lite Only	60
Standard Only	120
Professional Only	140
	Memory Requirement (Kbytes)
Lite & Standard Only	140
Lite & Professional Only	160
Standard & Professional Only	220
Lite, Standard & Professional	240

RMON is designed to grow and never free memory resources. We allow users to reserve memory to the RMON engine with the command " rmon set memory <memory in MB>". Users should allocate memory size based on the above table.

Per VLAN Spanning Tree (Spanning Forest)
Release 3.0 implements Spanning Tree per VLAN (also called Spanning Forest). A separate instance of Spanning Tree can be run per VLAN. On initialization, the SSR runs one spanning tree instance, which is called the default spanning tree (Note that this is backward compatible with pre-3.0 releases).

VLANs can run separate instances of Spanning Tree, or can be part of the default Spanning Tree instance. Although in theory each VLAN (up to 4093 VLANs) can have unique Spanning Tree instances, in practice it is advisable to have 30 Spanning Tree instances or less.

Per VLAN Spanning Tree is enabled on a per-port basis. If a port belongs to more than one VLAN and results in having more than one Spanning Tree instance, the user must specify which Spanning Tree instances are to be enabled on that port.

Load Balancing (LSNAT)
Load balancing allows you to use Network Address Translation in a "load sharing" capacity, where network traffic can be distributed across a pool of servers, rather than to a single server. Load balancing can be used by service providers and enterprise customers who need to balance traffic to a server farm.

If load balancing traffic is passing through ports that are configured for host-flow mode, no port translation takes place. Thus if you are using load-balance with host-flow mode, make sure that the destination server ports are the same as the virtual ports. Virtual groups performing FTP will not work in host-flow mode.

NAT
NAT is a feature that operates on a border router between an inside (local) network with private addressing scheme and an outside public (global) network with public addressing scheme. The translation functions in conjunction with other routing features, allowing for transparent access to the Internet from privatized remote hosts.

QoS Rate Limiting
QoS rate limiting is implemented on a per IP flow basis. Rate limiting is applied to an IP interface and not to a port. Rate limit takes effect on an input interface. The matching criteria for rate limiting are IP access lists. To set rate limits on a flow, the administrator needs to specify the rate in bits per second (bps) as well as the exceed action criterion. If the rate limit criterion is violated, then the following exceed actions can be performed: drop or lower the priority.

TOS Rewrite:
The TOS byte is part of the QoS priority classifier group. In the non-differential services model of TOS, the TOS byte is composed of three fields: the upper three bits represent the precedence, the next four bits represent the Type of Service; and the least significant bit is unused. These TOS bit fields can be independently changed by specifying them through the **qos set ip** command. When entering the **qos set ip** command, the ***tos-precedence-rewrite*** value affects only the upper three precedence bits, and the ***tos-rewrite*** value affects the lower four TOS bits plus the unused bit. To rewrite the entire contents of the TOS byte (for example, to convert from ***non-differential*** to ***differential service TOS***), use both the ***tos-precedence-rewrite*** value and the ***tos-rewrite*** value to change both bit fields of the TOS byte.

TOS-rewrite	*TOS-precedence-rewrite*	Action on TOS byte
X	Any	Replace lower 5 bits with X; preserve upper 3 bits from packet
Any	Y	Replace upper 3 bits with Y; preserve lower 5 bits from packet
X	Y	Replace all bits with values X and Y

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

Transparent Web Cache Redirect
The web cache redirect feature on the SSR works in conjunction with a cache server to store commonly accessed HTTP objects locally on the cache server. This results in substantial cost savings by saving on WAN access costs and increasing the response time tremendously. This feature offers redundancy and load sharing capabilities for building high availability cache server farms. Web caching is transparent to the user.

The **web-cache set maximum connections** command is currently not supported.

Per Protocol VLANs
In addition to IP and IPX, the protocols supported by SSR for protocol based VLANs are IPv6, DEC, SNA and AppleTalk. Note: Only IP and IPX can be routed by the SSR.

DHCP (Dynamic Host Configuration Protocol) Server
DHCP Server on the SSR provides dynamic address assignment and configuration to DHCP capable end-users. The SSR DHCP Server can provide a dynamic IP address from a pre-allocated pool of IP addresses or a static IP address. The SSR DHCP server is not designed to work as primary DHCP server in an enterprise environment. Please refer to "Known Restrictions and Limitations" for the SSR DHCP Server limitations.

Telnet Client
The SSR 's telnet client allows users to telnet from a SSR system CLI into other SSRs or systems to perform remote configuration. Only one active telnet session from the SSR is allowed at a time.

ICMP Router Discovery Messages
ICMP Router Discovery Messages enable hosts to discover the existence of neighboring routers. A periodic multicast advertisement is sent announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening to the advertisement.

Established Bit ACL
Established Bit ACL is an enhancement to the existing ACL feature. It allows network administrator to either permit or deny TCP connections being "established". Established Bit ACL can only be enabled from the TCP ACL configuration. The network administrator then applies this ACL to the IP interface.

HARDWARE REQUIREMENT:

The following table shows the hardware requirement for the specific features supported in this release:

SSR Feature Set		
SSR Part Number	Weighted Fair Queuing	Network Address Translation Load Server Balancing (LSNAT) Per Flow Rate Limiting Per Protocol VLAN Established Bit ACL TOS Rewrite
SSR 2000 / 2100		
Non -AA		
SSR-2-B	**X**	
SSR-2-FX	**X**	

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

SSR Feature Set		
SSR Part Number	Weighted Fair Queuing	Network Address Translation Load Server Balancing (LSNAT) Per Flow Rate Limiting Per Protocol VLAN Established Bit ACL TOS Rewrite
SSR-2-LX		
SSR-2-LX70		
SSR-2-PKG	X	
SSR-2-SER	X	
SSR-2-SERC	X	
SSR-2-SERCE	X	
SSR-2-SX		
SSR-2-TX	X	
-AA		
SSR-2-GSX		X
SSR-2-B-AA	X	X
SSR-2-FX-AA	X	X
SSR-2-PKG-AA	X	X
SSR-2-LX-AA		X
SSR-2-LX70-AA		X
SSR-2-SER-AA	X	X
SSR-2-SERC-AA	X	X
SSR-2-SERCE-AA	X	X
SSR-2-SX-AA		X
SSR-2-TX-AA	X	X
SSR 8000 / 86000		
Non -AA		
SSR-HTX12-08	X	
SSR-HTX22-08	X	
SSR-HFX11-08	X	
SSR-HFX21-08	X	
SSR-HFX29-08	X	
SSR-GSX11-02		
SSR-GSX21-02		
SSR-GLX19-02		
SSR-GLX29-02		
SSR-GLX70-01		
SSR-SERC-04	X	
SSR-SERCE-04	X	
SSR-HSSI-02	X	
-AA		
SSR-HTX12-08-AA	X	X
SSR-HTX22-08-AA	X	X

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

SSR Feature Set		
SSR Part Number	Weighted Fair Queuing	Network Address Translation Load Server Balancing (LSNAT) Per Flow Rate Limiting Per Protocol VLAN Established Bit ACL TOS Rewrite
SSR-HFX21-08-AA	X	X
SSR-HFX29-08-AA	X	X
SSR-GSX21-02-AA		X
SSR-GLX29-02-AA		X
SSR-GLX70-01-AA		X
SSR-SERC-04-AA	X	X
SSR-SERCE-04-AA	X	X
SSR-HSSI-02-AA	X	X

FIRMWARE CHANGES AND ENHANCEMENTS:

Resolved Issues

Issues Resolved in Version 3.0.1.0	I.D.
SSR did not respond to type "arpinarp" requests over frame relay. The SSR would not respond to ARP requests from a Bay router on which ARPINARP was set (the default. Inverse ARP replies from the SSR came back too late. The SSR now supports ARP Requests and replays. Inverse ARP replies are now sent more quickly using the correct DLCI in the reply target address.	07528
The miscalculation of the UDP checksum results in about a ten second delay before a DNS name gets resolved.	06641
Configurations for DHCP server with multiple DNS server addresses were not supported. A DHCP response can now contain up to 3 DNS server addresses.	08029
An improper message is printed when OSPF exits. When OSPF exits, the following messages are printed: "2000-01-21 15:02:06 %OSPF-E-NOROUTERID, Router ID is not defined. " "2000-01-21 15:02:06 %ERR-E-IVARGCNT, invalid argument count for error '20031540020SPF-E-EXIT'" Since the time-stamp is always printed by default, there is no need to have the time-stamp argument in the error message string."	07681 07682
Multicast – Some multicast applications were slow to restart or wouldn't restart when the SSR rebooted. This issue occurred with multicast applications where packets needed to be fragmented by IP. Separate flows were created for the packets that were fragmented from those that weren't. Creation of the fragment flow caused the long delay. This problem has now been corrected.	07832 06722
SAPinterval / RIPinterval – in early versions of the 3.0 firmware, it was not possible to change the default values for the SAPinterval / RIPinterval on more than one IPX interface at a time. This has now been corrected	07698

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

Issues Resolved in Version 3.0.1.0	I.D.
There have been problems accessing SSR MIBs from the SPEL MIB browser. In updating some of the supported MIB information, the agent instrumentation layer was not properly hooked up when the MIBs were changed. This issue has now been corrected.	08084
The NetScout RMON II application couldn't retrieve data from pprotocolDistStatsTable using the Get operator. An error in the original implementation of the protocolDistStatsTablerequires, which should have returned two arguments, returned only one to mdb_e_get(). This problem has now been corrected.	08083
High static memory allocation in Per-VLAN-Spanning-Tree (PVST) consumes a lot of memory that may initially be needed for PVST. The static allocation of memory has been reduced to a more reasonable value.	07848
The Virtual File System has been extensively modified (VFS v2) in this release of the firmware to improve Flash write performance. This feature requires boot prom version 1.1.0.8 and the flash memory must be reformatted to VFSv2.	07301 06281
Slow boot time – The boot time of the SSR has been reduced, for large configurations, by improving the efficiency of the CLI command merge operations.	07802
There was a security issue regarding telnet access to the SSR and was corrected in this version of the firmware.	07630
Layer 2 bridging over WAN interfaces - frames with the wrong source MAC address were generated for traffic routed to a VLAN containing a WAN port. The proper (SSR system) MAC address is now used for this type of traffic.	07794
Receiving a mal-formed bridge Protocol Data Unit (BPDU) on the WAN (frame relay) port of the SSR could result in an SSR core dump. This problem has now been corrected.	07628
load-balance - port translation results in wrong checksum - If the user set up a group with one virtual port and a different destination port (resulting in a port translation), the packets processed in software for the translation had the wrong checksum. This has been corrected.	07560
SNMP sysHwModuleTable – a core dump could occur when polling the sysHwModuleTable for a non-existent port. A check was added for null pointers before accessing the table value.	07542
Parts of the Layer 2 Bridge-MIB were never completed per rfc 1493. This MIB is now complete.	07193
SmartTrunks, traffic distribution – A core dump could occur on an SSR configured with a SmartTrunk using the "link utilization" distribution algorithm. This problem has now been corrected.	07541
When a serial card was configured in slot 1 of the SSR, instability in SmartTrunks could result. In some instances ports within the SmartTrunk would fail to operate. This problem has been corrected.	06555

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

Issues Resolved in Version 3.0.1.0	I.D.
Using SPEL - SNMP poll on the interface index (ifindex) caused the SSR to crash. Modifications to the interface index have been made to correct this problem.	
Multicast QoS specified with interface did not function properly. When a multicast QoS priority profile was defined for an interface, the multicast flow did not get the correct priority. This has now been corrected.	
In this version of the SSR firmware Investigation of memory leaks on the SSR, revealed several problems with memory alignment and memory allocation. These memory leaks have been eliminated.	07141
A memory leak was discovered related to configurations containing a syslog server . If the server was unreachable and a message was queued for delivery, the trap queue eventually exceeded maximum length and the SSR would lose 44 bytes of memory for every new message that was undeliverable. The problem has now been corrected.	07261
Memory leak would occur when command was enter and successfully executed through a telnet session while in configuration mode. This issue has been corrected.	07147
A memory leak would occur when multiple rip interfaces were created to the same remote LAN. The SSR would loose 6624 bytes of memory every 30 seconds. This situation has been corrected.	07203
WAN bridging – layer 2 frames inbound on a WAN port were not flooded out WAN ports in the same VLAN, on the same WAN module. This problem has been corrected.	07318
The SSR crashed with no crash dump after GATED-E-ASSERTFAIL messages. It was found that SNMP referenced all of the CIDR and OSPF mib-functions directly. This should have been an inter-process communication (IPC) mechanism, which sends a message to GateD to retrieve the MIB. This problem has been corrected.	07377
CLI terminal monitor failed to restore properly – If logged into the SSR via telnet and using 'cli terminal monitor', the telnet session would abruptly closed (by sending a FIN to the SSR). Console messages would no longer appear on the console or any subsequent telnet session. This condition could be resolved only by rebooting the SSR. This problem has now been corrected.	06850
The SSR would process LMIs on VC 1023, even though this VC was not defined. This was due to the fact that VC 0 & VC1023, are always defined, regardless of the type of LMI in use. This condition has been corrected, by creating only the VCs for the specified LMI type (e.g. 0 for annex A & D, 1023 for rev 1).	07135
The SSR failed to declare a link down when too many errors were encountered. The errors are now accounted.	07135
After failing to receive a response to a “Full Status Enquiry”, the SSR sends a “Link Integrity Verification”. The correct response should have been to continue to send “Full Status Enquiry” until the SSR received a satisfactory response.	07135

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

Issues Resolved in Version 3.0.1.0	I.D.
Within an LMI, the status for VCs 0 & 1023 should be disregarded. Generally, the network will not give status on these VCs since they are reserved for signaling. This problem has been corrected.	07315
In some instances, packets were getting dropped over frame-relay circuits, this was due to a Frame Checksum Error. This problem has been corrected.	06951
ip-policy stopped forwarding when the ARP cache was cleared. This has been corrected.	07182
The command "debug malloc health" crashed the SSR in some situations due to multiple tasks accessing the same data structures. The problem has now been corrected.	07222
“ipx show servers” command sometimes did not show the output. This problem has been corrected.	07427
“ipx show servers” sorted output was not displayed correctly . This problem has been corrected.	07501
LFAP experienced some performance issues in previous versions of code. This problem has been correctd.	07108
The SSR now sets the default ase-type for OSPF.	06928
Network Address Translation of DNS traffic resulted in a UDP checksum miscalculation, this problem has been corrected.	06641
Network Address Translation (NAT) was performing translation between two inside interfaces. This has been corrected.	06940
When copying the boot image on the SSR to the slave CPU, the console on the master CPU could hang. In addition, IP and OSPF could show some sluggishness. This behavior has been corrected.	06220
In some cases the ACL statistics reported by the SSR could be inaccurate. These statistics are now correct.	06953
The SSR could crash if a line card had been hotswapped out of the SSR, and then Corewatch was used to issue a query of the Modules Array. This problem has been corrected.	06434
In some cases, when Port Mirroring was enabled and an ICMP echo request was received on the SSR, immediately followed by an ARP request, the SSR could crash. This problem has been corrected.	06930
The SSR could core dump when an RMON query was issued for the hostTopN statistics. This problem has been corrected.	06942

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

Issues Resolved in Version 3.0.1.0	I.D.
When auto-negotiation was disabled on a gigabit port and no link was established, the red LED would flash intermittently. This behavior has been corrected.	06639
In some cases the SSR-2000 would hang during manufacturing diagnostics - this problem was usually experienced during flash write operations. This problem has been corrected.	06896
When the SSR is configured with both flow and destination mode forwarding for bridged traffic (L2) a core dump could occur during address/flow deletion. This problem has been corrected.	06062
SSR configuration errors could occur when a line card containing all or part of a SmartTrunk was hotswapped out and then put back into the SSR. This problem has been corrected.	06064
The RMON utilization – SSR reported incorrect network utilization statistics for ports running at speeds greater than 10 megabits per second. These statistics now indicate a more accurate representation of the network traffic.	06777

KNOWN RESTRICTIONS AND LIMITATIONS:

Hardware

100Base-FX Module

Using a single power supply (part number - 200-003-01 rev A), a maximum of five 100Base-FX modules can be installed in an SSR 8000 chassis, provided the other two slots are empty. If an SSR 8000 is to be configured with more than five 100Base-FX modules, the SSR 8000 must also be configured with two power supplies, otherwise it may not be able to boot.

Alternately, the SSR 8000 can be configured with the new power supply (part number - 200-003-02 rev 0A), capable of powering an SSR 8000 configured with up to seven 100Base-FX modules.

1000Base-SX/LX Module

If you are connecting the 1000Base-SX/LX module to another device that does not support auto negotiation, then link negotiation mode on both devices should be turned off. Be sure that both devices are set to the same link negotiation mode.

Weighted Fair Queuing (WFQ) is not supported on 1000Base-SX/LX/LX70 modules.

100Base-TX Module

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

100Base-TX Module

In some instances, if a 100Base-TX module is configured to auto negotiate, link failure may occur due to incorrect implementation of the auto negotiation feature by the device. The workaround is to manually set the port speed and duplex settings on the SSR.

Control Module

If you are using an SSR-CM2-64/128 Control Module, you must place the PCMCIA flash card in slot0. Slot0 is the top PCMCIA slot on the Control Module.

A Control Module memory upgrade is recommended if the SSR reports the error message: **SYS-E-MEM 95%of heap memory used**. This condition may occur when the SSR is deployed in a configuration having many Layer-2 MAC Addresses, Layer-3 flows, routing table entries and ports with RMON/RMON2 enable.

The SSR 8600 requires the new SSR-CM2-64/128 Control Module. If you use the old SSR-CM-64/128 Control Module with the SSR 8600, it will not boot.

Power Supply Trap

When one power supply is powered down, some power fluctuation may occur. Although this fluctuation is not a problem, it may result in the triggering of multiple traps.

SSR 2000

The SSR 2000 does not support a configuration consisting of two Gigabit modules or two 100Base-FX modules.

WAN Modules

The WAN hardware does not provide internal clocking. A CSU/DSU combination is required for packet framing.

KNOWN RESTRICTIONS AND LIMITATIONS:

Firmware

Telnet

Telnetting from SSR_1 to another SSR (SSR_2) and then back to SSR_1 might result in a lock-up both SSRs, during the execution of some commands.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

Telnet

During the telnet session, if the "Ip show routes" command is executed, on and SSR with a large number of entries in the Routing Information Base, the SSR might crash. This issue will be addressed in the next release of the firmware.

802.1Q

If a trunk port is created, the port is changed from access to trunk, but is not automatically added to any VLAN. Use the **vlan add port** command to add the trunk port to required VLANs.

Before a port is made part of an 802.1Q trunk, it cannot be assigned to any VLANs other than the default. You must make the port into a trunk port before adding VLANs to the trunk port.

Access Control Lists

The "implicit deny rule" is applied differently to an ACL for IPX than it is to an ACL for IP. If an ACL is defined for IP, the implicit deny rule denies all traffic. You must then explicitly permit traffic as desired. IPX ACLs are applied by traffic type. Consequently, the implicit deny rule applies only to the traffic type specified in the ACL. All other IPX traffic types are unaffected.

Bridging

Under some circumstances, SNA/DLC/NetBIOS traffic is not properly bridged across the SSR. The issue in bridging DLC packets occurs where the length field within an IEEE 802.3 frame indicates less than 46 bytes of data.

The SSR removes the length field information of incoming IEEE 802.3, 802.2, or Ethernet_Snap packets and recalculates the field prior to retransmission. Consequently, this calculation is based on the entire length of the data field. A packet entering the SSR with a length field indicating a data field of less than 46 bytes will exit with the length field recalculated incorrectly. This can be a problem with LLC2 and legacy IPX applications. Typically, such packets exist only in SNA and NetBIOS/NetBEUI environments.

Additional information can be found in Technical Tip - TK0310-9, January 13, 1999 at:
http://www.cabletron.com/support/techtips/tk0310-9.html

BGP

The **bgp show route default** command shows all routes, rather than just the default route.

NAT

Configuring VRRP on NAT interfaces is currently not supported.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CPU Redundancy
You cannot hot swap an active Control Module without pressing the HotSwap button or operating through the console. Doing so will cause the SSR to crash.
If the backup Control Module fails to receive a heartbeat from the active Control Module for a certain interval (~60 seconds), the backup Control Module assumes the active Control Module's role, including its MAC address. If you repair or replace the non-functional Control Module and then reboot the SSR, the new Control Module will have a different MAC address.
The Power On Self Test (POST) fails if a redundant Control Module is installed. The workaround is to make only one Control Module active when the POST is enabled. Either install only one Control Module or do not load software on the redundant Control Module.

DHCP
The **DHCP global set ping-timeout <number>** command is currently not supported.
The DHCP server currently ignores packets arriving on PPP MLP interfaces.
The DHCP server currently cannot specify a Bootp server address to be sent to clients.
The following commands are not supported in the 3.0 firmware release. **dhcp scope-name set ping-timeout <number>** **dhcp scope-name set lease-database <url>** **dhcp scope-name set commit-interval <number>**
When configuring DHCP to use RCP or TFTP, make sure that the RCP/TFTP remote host address and password syntax is specified correctly. This address is not validated by the CLI. Therefore the RCP/TFTP will fail if the address or password is incorrectly specified, and an error message will appear on the console.
If DHCP configuration is negated before lease expiration, the **dhcp show** command (in enable mode) shows incorrect information.
The maximum number of address can be served by the SSR DHCP server is 253.

DVMRP

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

DVMRP
If an interface that has DVMRP or IGMP enabled is deleted and added back again, DVMRP and IGMP do not detect it. The workaround is to restart DVMRP by executing the **no dvmrp start** command and committing the change, then executing the **dvmrp start** command and committing the change.
DVMRP scope does not work in this current release of the firmware.
A multicast packet is replicated to only one IP VLAN in an 802.1Q trunk port. Instead of an 802.1Q trunk port, you should use an access routed interface to forward multicast packets between two SSRs.

IP Routing
The en0 (Ethernet port on the Control Module) is a management port only and is not intended to and does not perform routing.
The **globals**, **timers**, **interfaces**, **active-gateways**, **interface-policies**, **import-policies** and **export-policies** options for the **rip show** command do not work. However, you can obtain this information by entering the **rip show all** command.
The default value of the OSPF hello-interval for virtual links has been changed to 10 seconds from 60 seconds.
A maximum of 120 RIP interfaces can be created on an SSR.
The ip-hash load balancing method in policy routing has a known problem. If the gateway where traffic is supposed to go through is down, the traffic will go to one of the active gateways according to the sequence when the gateway becomes available. This is not according to the sequence specified in the user configuration.
The **ip-policy show interface all** command does not show the ip-policy from the interface point of view. It shows the ip-policy that is applied to all interfaces. If there are 20 interfaces, but no ip-policy applied to all interfaces, then **ip-policy show interface all** command will return **%PBR-I-NOALL, No policy applied to all IP interfaces.** The output would be shown only if there is a policy applied to all interfaces.
In the ip-policy definition, if a load-balancing policy is defined for a policy which needs to be changed, the old load balancing policy needs to be negated before defining a new load balancing policy. SSR does not replace the old policy with the new one without explicit removal of the previous policy.
To ensure availability of a gateway that is used for policy routing, enable the pinger task.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

IP Routing

If there is a redistribute or export-related policy command in the configuration, such as the following:

ip-router policy redistribute from-proto ospf to-proto rip

then the default policies are superseded; that is, RIP and direct routes are no longer redistributed by default. To redistribute RIP and direct routes that would have been announced by default policies, you must explicitly redistribute them. For example:

ip-router policy redistribute from-proto direct to-proto rip
ip-router policy redistribute from-proto rip to-proto rip

When defining the default route, the CLI accepts the IP address of 0.0.0.0. But unless the mask is included (0.0.0.0/0), the route will not work.

IPX Routing

A maximum of 64 IPX interfaces can be created on an SSR.

Multiple IPX encapsulation types are not supported in version 3.0.

Port Statistics

The **statistics show port-stats** command does not reflect correct one-minute traffic rates.

The Frame count for layer-2 MAC broadcast frames in the port statistics menu is incorrectly counted twice.

Packets less than 64 bytes in length are incorrectly counted as either CRC or Alignment errors instead of Runt Packet errors.

The statistics counters for IP, ICMP, UDP and TCP cannot be cleared to conform to the SNMP standard.

Proxy ARP

When creating an IP interface, the **ip interface create** command requires a logical name for each interface. If you use a name that begins with **en** or **lo**, it causes the SSR to disable the proxy ARP on those IP interfaces.

Quality of Service (QoS)

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

Quality of Service (QoS)

The **interface name** parameter, which is the last possible parameter when configuring an IPX QoS entry, does not work. Do not enter an interface name when configuring an IPX QoS entry.

Certain L2 QoS configurations may not work when applied to a port set to **flow-bridging** mode. (The default setting for a port is **address** mode.) The situation typically is found in a lab-test environment where two stations are sending traffic to each other (and to no one else) through an SSR configured so that the ports are in flow mode, and where QoS entries apply to their bi-directional traffic. This results in packets always going through the CPU and, consequently, degraded performance.

RMON

The **no** command does not work on RMON commands in the active configuration. When it is necessary to remove an RMON command from an active configuration and replace it with a new RMON command, you must reboot the SSR to make the new RMON command take effect.

The RMON agent currently only reports the traffic received on a port. This affects etherstats, packet capture, and all of the RMON tables. The cumulative RMON data in the SSR reports correct information of all of the enabled ports, but looking at a single port for data does not show the exiting traffic.

Packet capture using RMON should be done with care. Whenever packet capture is enabled, it takes up considerable CPU cycles. Run packet capture provided that the CPU is not busy running other important tasks and CPU utilization is low.

Routed traffic will NOT be accounted for in RMON1 host and matrix statistics.
Bridged traffic will NOT be accounted for in RMON2 host, matrix, and protocol distribution statistics.

Any WAN traffic received on a WAN port will be reflected only on the first physical port of the module.

rmon show status command will display the wrong amount of memory allocated whenever the user changes the memory allocation.

SmartTRUNKs

When Huntgroup protocol is enable on SmartTrunk and if the Control Module is too busy to send or receive Huntgroup PDUs, SmartTRUNK links may be affected.

If a SmartTRUNK has been configured to carry traffic for an IP VLAN and you want to have it carry traffic for the L2 default VLAN as well, you must make the SmartTRUNK into an 802.1Q trunk, then disable and enable the SmartTRUNK.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

SmartTRUNKs

When a hotswap is performed on any card, the link for any SmartTrunk configured with huntgroup protocol goes down for a few seconds.

If you hotswap a card that has SmartTrunk configured along with Layer 2 filters, then the SmartTrunk commands are marked with an "**E**".

SNMP

Get-next on the capMemoryTable returns no response, although the capMemoryTable has been traversed completely.

Values in capCPUTable obtained via SNMP and values displayed by the **system show capacity** command do not agree. CapCPUTable obtained by SNMP displays all tasks correctly.

A **get** on the capMemoryRemovable object returns an incorrect value.

The following MIBs are not supported in the current release:

VLAN-MIB.txt	- experimental status in IETF
DVMRP-MIB.txt	- experimental status in IETF
IGMP-MIB.txt	- experimental status in IETF
OSPF-MIB.txt	RFC 1850
OSPF-TRAP-MIB.txt	RFC 1850
RIPv2-MIB.txt	RFC 1724
BGP4-MIB.txt	RFC 1654 - **Note:** BGP traps work in 3.0 regardless of MIB enabled status

Spanning Tree Protocol

When using the **stp enable port** command for virtual port on WAN module for a list of virtual ports, only the first virtual port will be enabled.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

SSR 8600 Firmware

If you need to downgrade the SSR 8600's system firmware from version 2.x.x.x code to version 1.2.x.x, make sure to power down the SSR and power up again before downgrading system firmware. If you do not do this, the SSR may not be operational, or you may see the following error message:

SYS_ERR: Transmit queue full

Additional information can be found in Technical Bulletin:
http://www.cabletron.com/support/techbltn/tb0806-9.html

STATISTICS SHOW SUMMARY-STATS

The output for the "statistics show summary-stats" command provides erroneous information for 5-minute and 15-minute summaries until the system uptime exceeds these time intervals.

System

CLI commands cannot be executed if a Telnet session is started via rsh from a UNIX system.

Updating and erasing the system firmware image should not be done simultaneously.

If you are using SSR-CM-64/128 Control Modules, network performance on the network management port (en0) may become slower than normal under certain circumstances. The workaround is to use one of the other network ports, e.g., et.2.1 to perform tasks such as upgrading the firmware image or Telnet.

The local file system on the SSR currently does not fully support filenames with mixed or uppercase characters. Please use filenames with **only** lowercase characters.

If a line card is removed without first issuing the command "system hotswap out slot x", the SSR will core dump. A core dump will also occur if the module is removed before the hot swap operation has completed.

VLANs

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

VLANs

There are two special VLANs on the SSR, the Default VLAN (ID=1) and the VLAN with ID=4095. The Default VLAN contains all of the ports not used in other VLANs. When ports are added to VLANs, they are removed from the Default VLAN. When ports are removed from a VLAN with an ID other than 1, they are returned to the Default VLAN. The VLAN with the ID of 4095 (a.k.a. the "blackhole VLAN") is used as the repository for all incoming frames with no destination.

These two VLANs have the following restrictions:

- Ports cannot explicitly be added to either of these VLANs.
- Layer 3 interfaces cannot be associated with "Blackhole VLAN" (ID = 4095)
- IPX interfaces cannot be associated with "Default VLAN" (ID = 1).

TACACS/RADIUS

The **system show users** command does not show the names of users that have been authenticated through TACACS or RADIUS.

Time of Day Clock

After setting the clock on the SSR and then clearing the port statistics, the time-of-day clock may be reset to its time as well.

WAN Modules

The maximum allowed MTU size for WAN interfaces is 1500 bytes and cannot be changed.

If WAN ports are in the default VLAN, L2 traffic does not bridge on the WAN ports.

A configuration with an IPX interface used in a VLAN containing both LAN and WAN ports is not supported.

IPX is not supported in partially meshed WAN networks if nodes are using the same network address. Different IPX network addresses should be used for each node of the network.

Port mirroring, ACL, and L2 filtering is supported on a per-WAN-card basis, not on a per-port basis.

For PPP, IPX Network numbers for both the local and peer router must be the same. Mismatched network numbers may cause routing and other problems.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

WAN Modules
STP (Spanning Tree Protocol) per VLAN (PVST) is not supported on WAN ports.
Packets do not flood WAN ports belonging to the Default VLAN. To allow flooding of packets, the WAN port should be added to a non-default VLAN.

CoreWatch Software

Information about CoreWatch is covered in a separate Release Note. The latest ***CoreWatch User's Guide*** is located on the CoreWatch CD.

Any problems other than those listed above should be reported to our Cabletron Technical Support Staff.

ERRATA:

The following are corrections to the following documentation:

SSR Command Line Interface Reference Manual - p.463:
nat create dynamic local-acl-pool <local-acl> **global-pool** <ip-addr/ip-addr-range/ip-addr-list/ip-addr-mask> **[matches-interface** <interface>**][enable-ip-overload]** **nat flush-dynamic-binding all | pool-specified [local-acl-pool** <local-acl>**] [global-pool** <ip-addr/ip-addr-range/ip-addr-mask>**]**

SSR Command Line Interface Reference Manual - p.640:
ssr(config)# rdisc add address 10.20.36.1

SSR Command Line Interface Reference Manual - p.643:
ssr#(config) rdisc set address 10.20.36.1 type broadcast

SSR Command Line Interface Reference Manual - p.645:
"To specify the value for the maximum time between the sending of router advertisement on an interface:"

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

COMPLIANCE SUPPORT:

Compliance Level	Compliant
Year 2000	Yes

Known Anomalies: None.

IEEE STANDARDS SUPPORT:

Standard	Title
IEEE 802.1d	Spanning Tree
IEEE 802.1p	Traffic Prioritization
IEEE 802.1Q	VLAN Trunking
IEEE 802.3	10 Mbps Ethernet
IEEE 802.3u	100Base-T Ethernet
IEEE 802.3x	Full Duplex Ethernet
IEEE 802.3z	1000 Mbps Ethernet

IETF STANDARDS SUPPORT:

RFC No.	Title
RFC 1058	RIP v1
RFC 1105	BGP
RFC 1157	SNMPv1
RFC 1163	BGP-2
RFC 1213	MIB-2
RFC 1253	OSPF v2 MIB
RFC 1256	ICMP Router Discover Message
RFC 1265	BGP Protocol Analysis
RFC 1266	Experience with the BGP Protocol
RFC 1267	BGP-3
RFC 1293	Inverse ARP
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1349	Type of Service in the Internet Protocol Suite
RFC 1397	BGP Default Route Advertisement
RFC 1490	Multiprotocol Interconnect over Frame Relay
RFC 1519	CIDR
RFC 1548	The Point-to-Point Protocol (PPP)
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1570	PPP LCP Extensions
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1583	OSPF v2
RFC 1631	IP Network Address Translator
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1656	BGP-4 Protocol Document Roadmap and Implementation Experience
RFC 1657	BGP-4 Definitions of Managed Objects
RFC 1661	PPP (Point-to-Point Protocol)

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

RFC No.	Title
RFC 1662	PPP in HDLC-like Framing
RFC 1723	RIP v2
RFC 1771	BGP-4
RFC 1772	Application of BGP in the Internet
RFC 1812	Router Requirements
RFC 1966	BGP Route Reflection
RFC 1990	PPP Multi-Link Protocol
RFC 1997	BGP Communities Attribute
RFC 2096	IP Forwarding MIB
RFC 2131	Dynamic Host Configuration Protocol
RFC 2236	Internet Group Management Protocol, Version 2
RFC 2391	Load Sharing using IP Network Address Translation (Load Balance)

IETF STANDARDS MIB SUPPORT:

RFC No.	Title
RFC 1471	PPP LCP (Link Control Protocol)
RFC 1472	PPP Security Protocol
RFC 1473	PPP IP NCP (Network Control Protocol)
RFC 1474	PPP Bridge NCP
RFC 1493	Definitions of Managed Objects for Bridges
RFC 1643	Ethernet Like Interface MIB
RFC 1654	BGP4 MIB
RFC 1724	RIPv2 MIB
RFC 1757	Remote Network Monitoring (RMON) Management Information Base
RFC 1850	OSPF and OSPF Trap MIB
RFC 2011	Internet Protocol using SMIv2
RFC 2021	Remote Network Monitoring Version 2 (RMON 2)
RFC 2096	IP Forwarding MIB
RFC 2115	Frame Relay DTE using SMIv2
RFC 2233	Interfaces Group using SMIv2
RFC 2271	SNMP Management Frameworks
RFC 2618	Radius Authentication Client

IETF EXPERIMENTAL MIBS SUPPORT:

Function	Draft
DVMRP	Draft-ietf-idmr-dvmrp-v3-06.txt
802.1Q VLAN	IEEE Draft Standard P802.1Q/D9
IGMP	Draft-ietf-idmr-igmp-mib-11.txt

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

IETF STANDARDS SNMP TRAP SUPPORT:

RFC No.	Title
RFC 1157	linkDown, linkUp, authenticationFailure Traps
RFC 1493	newRoot, topologyChange Traps

FRAME RELAY STANDARD SUPPORT:

Standard	Title
Frame Relay Forum FRF.1.1	User-to-Network (UNI) Implementation Agreement
Frame Relay Forum FRF.3.1	Multiprotocol Encapsulation Implementation Agreement
ITU-T Q.922/ANSI T1.618	ISDN Core Aspects of Frame Relay Protocol
ITU-T Q.933	Access Signaling Annex A
ITU-T I.122/ANSI T1S1	Standards-Based Frame Relay Specification
ITU-T Annex D/ANSI T1.617	Additional Procedures for PVCs Using Unnumbered Information Frames

CABELTRON PRIVATE ENTERPRISE MIB SUPPORT:

Title	Description
Novell-ipx-mib	Novell Netware
Ctron-oids	Defines 52 ctron
Ctron-mib-names	Defines branches for lfap mib
Ctron-ssr-smi	Defines branch for ssr 2501
Ctron-ssr-hardware	Device specific hardware objects
Ctron-ssr-policy	L2 filters, l3 acls set/get ability
Ctron-ssr-service-status	Status of major subsystems
Ctlfap-mib	Flow accounting system status
Ctron-ssr-capacity	New with 3.0 use for performance/capacity
Ctron-ssr-config	Retrieve/send configuration file via tftp
VRRP-MIB	VRRP Draft #8
Novel-rip-sap-mib	Novell Netware RIP SAP

Cabletron Private Enterprise MIBs are available in SMI v1/v2 format from the Cabletron Web Site at:

http://www.cabletron.com/support/mibs/

Indexed MIB documentation is also available.

GLOBAL SUPPORT:

By Phone: (603) 332-9400
By Email: support@cabletron.com
By Web: http://www.cabletron.com/support
By Fax: (603) 337-3075
By Mail: Cabletron Systems, Inc.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

CUSTOMER RELEASE NOTES

P.O. Box 5005
Rochester, NH 03867-5005

For information regarding the latest firmware available, recent release note revisions, or if you require additional assistance, please visit the Cabletron Support Web Site.

35 Industrial Way
PO Box 5005
Rochester, NH 03867-5005
(603) 332-9400

Appendix - Issues resolved in previous firmware releases

Issues Resolved in Version 3.0.0.2
Reverse ARP (RARP): Memory was consumed as RARP messages arrived at the SSR CPU. This problem occurred when an IP interface was created and RARP was disabled on that interface (the default condition) or if there was no mapping of the MAC address to an IP address in the RARP table.
Spanning Tree and WAN interfaces: In version 3.0.0.0, the SSR could core dump in STP when the WAN interface was configured with more than 128 virtual circuits.
Server load balancing issue: LSNAT continued to ping a host that had been removed from a load-balance group.
IP Multicast issue: Requests from clients did not reach the Server - this problem was caused by an internal queuing mechanism in the IP Multicast software.
IPX RIP Request - memory corruption: A memory corruption issue was found to occur when the SSR received large IPX RIP requests.
BGP: The command to show all of the routes advertised by BGP did not display all of the routes.
SmartTrunk and Hotswap: Hotswapping out a portion of a SmartTrunk caused a problem in the operation of the remaining links within the SmartTrunk. During the Hotswap operation, if a "Port Up" event occurred before the Hotswap operation completed, the Hotswap task would go into a bad state. This problem was corrected by insuring that the Hotswap operation is always completed before a "Port Up" condition is set.
ACL and alternate forwarding modes: Incorrect ACLs were installed when the SSR was in Host/Destination L3 mode.
BGP Trap memory management problem: Memory allocated by Gated was given to the SNMP task, which in turn freed it after sending a trap. Gated would then attempt to free the same memory, resulting in a system crash.
Power-On Diagnostics: A problem was found and fixed in the diagnostic routines for the 4 port serial card.

End of Release Notes